

The Automorphism Group of an [18, 9, 8] Quaternary Code*

*Ying Cheng***

Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974

I. Introduction

An [18, 9, 8] code #₁₈ over $GF(4)$ was constructed in [6] as an extended cyclic code, and Pless [9] describes the same code as an extended “ Q -code”. This code is of particular interest since it is an extremal quaternary code: an $[n, n/2, d]$ self-dual code with $d = 2\lfloor n/6 \rfloor + 2$ ([6, p. 295], [3, p. 205]).

In the present note we give new coordinates for this code, enabling us to find a simple description of its 2754 minimal weight words and also to determine for the first time its automorphism group G . This group G has structure $3 \times (PSL_2(16).4)$ and order 48960, and has two orbits on the coordinates, of sizes 17 and 1.

It is interesting that, although G is not transitive on the 18 coordinates, the [17, 9, 7] punctured codes obtained by deleting any one coordinate all have the same weight enumerator, and even the same complete weight enumerator.

* This appeared in “Discrete Math.”, vol. 83 (1990), pp. 205–212.

** Supported in part by a grant from the Louisiana Educational Quality Support Fund.
Present address: AT&T Bell Laboratories, Holmdel, NJ 07733.

We also study the properties of the particular $[17, 9, 7]$ code $\#_{17}^{(9)}$ obtained by puncturing the 18th coordinate (the odd-man-out), and its even subcode $\#_{17}^{(8)}$, which is a $[17, 8, 8]$ code. Two other cyclic codes also appear: a $[17, 4, 12]$ code $\#_{17}^{(4)}$, which is a two-weight code studied by Calderbank and Kantor [1], and its dual, which is a $[17, 13, 4]$ code $\#_{17}^{(13)}$. The codewords of maximal weight in $\#_{17}^{(4)}$, taken modulo scalar multiples, form a complex conference matrix (see Fig. 4).

These four codes of length 17 may also be constructed from 17-dimensional lattices that arise from Plesken's classification of the maximal groups of 17×17 integer matrices [8]. It is shown in [4] that certain of these lattices have a natural description using complex coordinates belonging to the set $\# = \{a + b\omega : a, b, \in \mathbb{Z}, \omega = e^{2\pi i/3}\}$ of Eisenstein integers. By using the isomorphism $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \cong GF(4)$ ([3, p. 199]), these lattices project onto codes over $GF(4)$. In fact the lattices $Q_{17}(6)$, $Q_{17}(6)^{+2}$ and $Q'_{17}(6)$ of [4], with automorphism group $2 \times (PSL_2(16).4)$, project in this way onto the codes $\#_{17}^{(8)}$, $\#_{17}^{(9)}$ and $\#_{17}^{(4)}$ respectively.

In the following section we establish our coordinate system and define the group, and then the codes are defined in Sect. III. We hope the reader will agree that these codes now look very simple (see especially Fig. 3).

The definitions of dual code and automorphism group for quaternary codes vary from author to author. The field automorphism of $GF(4) = \{0, 1, \omega, \omega^2 = \bar{\omega}\}$ takes $x \in GF(4)$ to $\bar{x} = x^2$ (and interchanges ω and ω^2). In this paper we use the hermitian inner product $(u, v) = u \cdot \bar{v} = \sum u_i \bar{v}_i$, and define the dual code $\#^\perp = \{u : (u, v) = u \cdot \bar{v} = 0 \text{ for all } v \in \#\}$. We take the typical element of the

automorphism group $\text{Aut}(\#)$ of $\#$ to consist of a permutation of the coordinates, followed by multiplication of the individual coordinates by nonzero field elements, and (possibly) conjugation of the whole vector. For any undefined terms see [2], [3] or [7].

II. Coordinates and group

We construct the field $GF(16)$ as in [4] by adjoining to $GF(2)$ an element ε satisfying $\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$ (a non-primitive polynomial!). If we define $\omega = \varepsilon + \varepsilon^4$ then $\omega^2 = \bar{\omega} = \varepsilon^2 + \varepsilon^3$, $\omega^2 + \omega + 1 = 0$, and $\varepsilon\omega$ is a primitive element of $GF(16) = \{0, \varepsilon^i \omega^j : 0 \leq i \leq 4, 0 \leq j \leq 2\}$. Furthermore $\{0, 1, \omega, \bar{\omega}\}$ is a copy of $GF(4)$ contained in $GF(16)$.

The codewords of $\#_{18}$ are vectors with 18 coordinates labeled $\{x_t : t \in GF(16), x_\infty, x_\Omega\}$, arranged in an array as shown in Fig. 1a. For the codes of length 17 we omit x_Ω .

The 4×4 block of coordinates in Fig. 1a forms an addition table for $GF(16)$. For example the sum of ε (at the top of a column) and ε^2 (at the left of a row) is $\varepsilon^4 \bar{\omega}$ (at the intersection of that row and column). Similarly $\omega + \varepsilon = \varepsilon^4$, $\varepsilon^2 + \varepsilon^4 \omega = \omega$, etc.

These coordinates have the advantage that the generators of the group and the minimal vectors of the codes look nice, but the disadvantage that the element of order 17 in the group is messy.

We now *define* G to be the group generated by multiplication of all coordinates by ω :

$$x_r \longmapsto \omega x_r ,$$

and by the maps α_t, β_t ($t \in GF(16)$), γ and σ , where

$$\begin{aligned}
 \alpha_t : x_r &\longmapsto x_{r+t} \quad (r \in GF(16)), x_\infty \text{ and } x_\Omega \text{ fixed,} \\
 \beta_t : x_r &\longmapsto \chi(t)x_{rt} \quad (r \in GF(16)), x_\infty \longmapsto \overline{\chi(t)} x_\infty, x_\Omega \longmapsto x_\Omega, \\
 \gamma : x_r &\longmapsto \chi(r)x_{1/r} \quad (r \in GF(16) \cup \{\infty\}), x_\Omega \longmapsto x_\Omega, \\
 \sigma : x_r &\longmapsto x_{r^2} \quad (r \in GF(16)), x_\infty \text{ and } x_\Omega \text{ fixed,}
 \end{aligned}$$

and $\chi : GF(16) \cup \{\infty\} \longrightarrow GF(4)$ is given by

$$\chi(\infty) = \chi(0) = 1, \quad \chi(\varepsilon^i \omega^j) = \omega^j,$$

except that when applying σ we must also conjugate all coefficients. The actions of α_ε , β_ω , β_ε , γ and σ are displayed in Figs. 1b-1f. The element $\delta = \alpha_\varepsilon \gamma$ (first α_ε then γ) has order 17 and is displayed in Fig. 1g. The maps α_t , β_t and γ are standard generators for $PSL_2(16)$ (cf. [4, p. 268] or [2]), σ (of order 4) corresponds to the field automorphism of $GF(16)$ and extends the group to $P\Gamma L_2(16) = PSL_2(16).4$, and the scalar multiplications by 1, ω and ω^2 are in the center of the group. The order of G is therefore $3 \cdot 15 \cdot 16 \cdot 17 \cdot 4 = 48960$.

It is clear from Fig. 1 that G has two orbits on the coordinates, $\{x_t : t \in GF(16), x_\infty\}$ and $\{x_\Omega\}$, of sizes 17 and 1. We define G_Ω to be the group obtained from G by ignoring the x_Ω coordinate. Since all elements of G fix x_Ω (or multiply it by a scalar), G_Ω and G are isomorphic groups.

Remark. We can make the element δ of order 17 into a *permutation* of order 17 (not mentioning ω or $\bar{\omega}$) by multiplying the coordinates of every vector (componentwise) by the field elements shown in Fig. 2. The codes in Sect. III then become cyclic or extended cyclic codes, but the simplicity of the generators of the group and the codes is lost.

III. The codes

Since G is not transitive on coordinates, the code $\#_{17}^{(9)}$ is the most basic, and we construct it first. We define $\#_{17}^{(9)}$ to be the code generated by the images under G_Ω of the vector u_9 shown in Fig. 3a. Similarly we define $\#_{17}^{(8)}$, $\#_{17}^{(4)}$, $\#_{17}^{(13)}$ to be generated by the images under G_Ω of the vectors u_8 , u_4 , u_{13} shown in Figs. 3b, 3c, 3e respectively, and $\#_{18}$ by the images under G of the vector v_9 shown in Fig. 3f. The vector u'_4 in Fig. 3d is an alternative generator for $\#_{17}^{(4)}$. Note that the 1's in u_9 are located at positions $\infty, 0, 1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$ (compare Fig. 1a), and that v_9 differs from u_9 only in the addition of an over-all parity check in position Ω .

It is now easy to check (by computer) that the first nine ‘‘cyclic shifts’’ of u_9 under δ , i.e. the vectors $\delta^i(u_9)$ ($0 \leq i \leq 8$), are a basis for $\#_{17}^{(9)}$, yielding the generator matrix

$$M_9 = \begin{array}{|l} 11011010010001000 \\ 11001200200000330 \\ 01001220032010000 \\ 00001203000010212 \\ 00200200011310002 \\ 00020002000313302 \\ 20100000102303002 \\ 02010013100303000 \\ 10202010100003030 \end{array} \quad (2 = \omega, 3 = \bar{\omega}).$$

Furthermore $\#_{17}^{(9)}$ is a $[17, 9, 7]$ code over $GF(4)$ with weight distribution

$i :$	0	7	8	9	10	11
$A_i :$	1	1224	1530	10200	8160	51408
$i :$	12	13	14	15	16	17
$A_i :$	25704	85680	24480	45288	5661	2808

To find the minimal vectors in these codes it is best to work in the subgroup

$PSL_2(16)$ generated by the elements α_t , β_t and γ , and to count vectors *projectively*, i.e. up to scalar multiplication by 1, ω and $\bar{\omega}$.

The vector u_9 is visibly fixed by the elements β_ε and γ (see Fig. 1). These generate a subgroup H of $PSL_2(16)$ of order 10, and one can show that nothing else in $PSL_2(16)$ fixes u_9 , even projectively. Then the number of projectively distinct images of u_9 under $PSL_2(16)$ is $|PSL_2(16)|/|H| = 15 \cdot 16 \cdot 17/10 = 408$. These vectors and their multiples by 1, ω and $\bar{\omega}$ are the $3 \cdot 408 = 1224$ weight 7 codewords of $\#_{17}^{(9)}$. It follows that the group G_Ω acts transitively on the minimal weight codewords of $\#_{17}^{(9)}$.

Similarly, the code $\#_{17}^{(8)}$ is generated by $\delta^i(u_8)$ ($0 \leq i \leq 7$), and is a $[17, 8, 8]$ code, consisting of the even weight words of $\#_{17}^{(9)}$. As generators we may use either $\{\delta^i(u_8) : 0 \leq i \leq 7\}$ or alternatively the successive differences of the rows of M_9 . This is the dual to $\#_{17}^{(9)}$.

The only elements of $PSL_2(17)$ that fix u_8 projectively are the elements α_t for t in the top two rows of the 4×4 array (the support of u_8). These form a group of order 8, so u_8 has $15 \cdot 16 \cdot 17/8 = 510$ projectively distinct images. Thus the $3 \times 510 = 1530$ minimal weight codewords of $\#_{17}^{(8)}$ are in one orbit under G_Ω .

The code $\#_{17}^{(4)}$ is generated by either $\delta^i(u_4)$ or $\delta^i(u'_4)$ ($0 \leq i \leq 3$), and has generator matrix

$$M_4 = \begin{bmatrix} 00022002233113311 \\ 20100321112201202 \\ 02310013201322310 \\ 10232022312003033 \end{bmatrix} .$$

This is a $[17, 4, 12]$ code with weight distribution

$$\begin{array}{rcccc} i : & 0 & 12 & 16 \\ A_i : & 1 & 204 & 51 \end{array}$$

and is a member of the class TF3 of two-weight codes studied by Calderbank and Kantor [1]. The columns of M_4 specify an ‘‘ovoid’’ in $PG(3, 4)$ (see [1], [5]).

The subgroup of $PSL_2(16)$ fixing u_4 projectively is $H = \langle \alpha_t, \beta_t : t \in GF(16) \rangle$, of order $15 \cdot 16$. Thus u_4 has $15 \cdot 16 \cdot 17/15 \cdot 16 = 17$ projectively distinct images, (see Fig. 4), and the 3.51 weight 16 codewords of $\#_{17}^{(4)}$ belong to one orbit under G_Ω .

Figure 4 shows the vectors $\{\delta^i(u_4) : 0 \leq i \leq 16\}$, taken in the order which places the zeros down the main diagonal, as usual with the convention that $2 = \omega$, $3 = \bar{\omega}$. If we now interpret $\omega = e^{2\pi i/3}$ and $\bar{\omega} = e^{-2\pi i/3}$ as complex cube roots of unity we obtain a 17×17 matrix H_{17} with the property that $H_{17} \bar{H}_{17}^{tr} = 16 I_{17}$. This may be regarded as a complex (or quaternary) conference matrix (cf. [7, p. 55]).

The $[17, 13, 4]$ code $\#_{17}^{(13)}$ is dual to $\#_{17}^{(4)}$, and is generated by $\delta^i(u_{13})$ ($0 \leq i \leq 12$). The weight distribution is (in part) $A_0 = 1$, $A_4 = 1020$, $A_5 = 6120$, $A_6 = 32640$, ..., $A_{16} = 2856561$, $A_{17} = 504648$. The vector u_{13} is fixed (projectively) by the subgroup of $PSL_2(16)$ generated by α_ω and β_ω , a group of order 12. Thus the $3 \times 340 = 1020$ minimal weight words are in one orbit under G_Ω .

Finally $\#_{18}$ is obtained by adjoining a column of 1’s to M_9 (for the Ω coordinate). This is an $[18, 9, 8]$ extremal self-dual code over $GF(4)$ with weight distribution

$$\begin{array}{rcccccccc} i : & 0 & 8 & 10 & 12 & 14 & 16 & 18 \\ A_i : & 1 & 2754 & 18360 & 77112 & 110160 & 50949 & 2808 \end{array}$$

(as in [6, Table II]). There are two orbits of minimal weight codewords under G , the 1224 images of v_9 and the 1530 images of u_8 (supplemented with a 0 in the Ω coordinate), for a total of 2754.

It only remains to determine the automorphism groups of these codes. By construction, the automorphism groups of $\# \binom{k}{7}$ ($k = 4, 8, 9, 13$) contain G_Ω , and $\text{Aut}(\#_{18})$ contains G . In fact $\text{Aut}(\# \binom{k}{7}) = G_\Omega$, and $\text{Aut}(\#_{18}) = G$. For the codes of length 17 this can be deduced from the list of permutation groups given by Sims [10]. The alternating and symmetric groups are the only permutation groups on 17 letters that are larger than $PSL_2(16)$.4, and these do not fix our codes. Furthermore one can show that there is no larger monomial group that fixes these codes. For $\#_{18}$ we must also rule out the possibility that $\text{Aut}(\#_{18})$ acts transitively on the 18 coordinates. But if so then it would be doubly transitive on the coordinates, and A_{18} or S_{18} are the only possibilities.

Although the $[17, 9, 7]$ codes obtained by deleting any coordinate of $\#_{18}$ have the same complete weight enumerator, they are not isomorphic. For if they were, the extended codes would also be isomorphic, and this would make $\text{Aut}(\#_{18})$ transitive.

Acknowledgements

We would like to thank P. J. Cameron, J. H. Conway, W. M. Kantor and J. G. Oxley for helpful discussions. This paper owes a considerable debt to Ref. [4], where certain 17-dimensional lattices related to these codes are studied.

List of figure captions

Figure 1. (a) Labels for 18 coordinates used to describe the $[18, 9, 8]$ code $\#_{18}$. For the codes of length 17, omit the Ω coordinate. (b)-(g) Action of the group elements $\alpha_\epsilon, \beta_\omega, \beta_\epsilon, \gamma, \sigma, \delta$. In (c), (e), (f), (g) the indicated actions are to be performed *after* the permutation.

Figure 2. We may obtain cyclic or extended cyclic codes by multiplying vectors component-by-component by these field elements.

Figure 3. Generating vectors for (a) $\#_{17}^{(9)}$, (b) $\#_{17}^{(8)}$, (c) $\#_{17}^{(4)}$, (d) $\#_{17}^{(4)}$ again, (e) $\#_{17}^{(3)}$, (f) $\#_{18}$. In each case the code is spanned by the images of the indicated vector under the group G_Ω or G . In fact, if the code has dimension k , the first k images under the element δ suffice to generate it.

Figure 4. Matrix H_{17} formed from the (projectively distinct) codewords of weight 16 in $\#_{17}^{(4)}$, with the property that $H_{17} \bar{H}_{17}^{tr} = 16 I_{17}$. ($2 = \omega, 3 = \bar{\omega}$.)

$$H_{17} = \begin{array}{|l} 01111111111111111 \\ 10311212213231332 \\ 13011122231323123 \\ 11103222123133213 \\ 11130221232312331 \\ 31311023332213212 \\ 11222301131233132 \\ 31113330221321232 \\ 12212113023313231 \\ 22131211301223233 \\ 13132312330111222 \\ 23121132122013332 \\ 13231233111302212 \\ 22113213132330122 \\ 32312232131112033 \\ 21321312133322201 \\ 31223212311313320 \end{array}$$

Fig. 4

References

- [1] A. R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” *Bull. London Math. Soc.* **18** (1986), 97-122.
- [2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford Univ. Press, 1985.
- [3] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 1988.
- [4] J. H. Conway and N. J. A. Sloane, “Low-dimensional lattices II: Subgroups of $GL(n, \mathbb{Z})$,” *Proc. Royal Soc. London*, to appear.
- [5] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, 1968.
- [6] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane and H. N. Ward, “Self-dual codes over $GF(4)$,” *J. Combinatorial Theory*, **A 25** (1978), 288-318.
- [7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1979.
- [8] W. Plesken, “Finite unimodular groups of prime degree and circulants,” *J. Algebra* **97** (1985), 286-312.
- [9] V. Pless, “ Q -codes,” *J. Combinatorial Theory* **A 43** (1986), 258-276.

- [10] C. C. Sims, "Computational methods in the study of permutation groups," in *Computational Problems in Abstract Algebra*, edited J. Leech, Pergamon Press, Oxford, 1969, pp. 169-183.

The Automorphism Group of an [18, 9, 8] Quaternary Code*

*Ying Cheng***

Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974

ABSTRACT

An [18, 9, 8] extremal self-dual code over $GF(4)$ and related [17, 4, 12], [17, 8, 8], [17, 9, 7], [17, 13, 4] codes are investigated. Simple coordinates are given for these codes, and their minimal weight codewords and automorphism groups are determined. The groups are all isomorphic to $3 \times (PSL_2(16).4)$.

* This appeared in "Discrete Math.", vol. 83 (1990), pp. 205–212.

** Supported in part by a grant from the Louisiana Educational Quality Support Fund.
Present address: AT&T Bell Laboratories, Holmdel, NJ 07733.